The case for a scoped version of eduPersonEntitlement

In most federated scenarios, the simplest complete semantics of an entitlement assertion is a specification of 1) the entitlement as well as 2) the institution under whose auspices the entitlement is granted. This is analogous to the semantics of affiliation assertions in federated scenarios in which both the affiliation and the affiliated institution or unit need to be expressed. Scoped variants of eduPersonAffiliation and eduPersonEntitlement can express these semantics in a natural fashion. eduPersonScopedAffiliation is already part of the eduPerson specification. MACE-Dir now proposes to extend eduPerson by adding a new attribute, eduPersonScopedEntitlement. In values of eduPersonScopedEntitlement, the entitlement itself would be the substring up to the first "@" sign starting from the left. The institution under whose auspices the entitlement is granted would be specified by the remainder of the substring after the first "@" sign. It is recommended that institutions or units be represented by DNS names.

Example: eduPersonScopedEntitlement: urn:mace:wisc.edu:entitlement:myWebSpacePlus@uwec.edu

In federated scenarios, use of the unscoped counterpart attribute, eduPersonEntitlement, is discouraged.

NOTE: Implications for the common licensed resource eligibility stipulation:

When the entitlement value "urn:mace:dir:entitlement:common-lib-terms" appears in the unscoped version of the eduPersonEntitlement attribute, the educational institution that is party to the contract is identified by the issuer element of the containing SAML assertion (this is in accordance with the existing language at http://middleware.internet2.edu/urn-mace/urn-mace-dir-entitlement.html.

When the entitlement value "urn:mace:dir:entitlement:common-lib-terms" appears in the scoped attribute, eduPersonScopedEntitlement, the educational institution is identified by the substring after the first "@" sign.